THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

MISTY WILLIAMS, as an individual and on behalf of all others similarly situated, Plaintiff, vs. AON PLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Misty Williams ("Plaintiff") brings this Class Action Complaint against Aon PLC ("Aon" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including at least Social Security numbers, driver's license numbers, and/or benefits information (collectively, "personally identifiable information" or "PII").

2. According to Aon's website, it "is a leading global professional services firm providing a broad range of risk, retirement and health solutions."[1] Aon employs approximately 50,000 people across 120 countries and bills itself as "offer[ing] risk advisory, risk transfer and structured solutions that help organizations and individuals better identify, quantify and manage their risk exposure."[2] One such risk solution it claims to offer clients is that of cybersecurity.[3]

[1] https://www.aon.com/apac/about-aon/default.jsp
[2] https://www.aon.com/home/solutions/commercial-risk.html
[3] https://www.aon.com/cyber-solutions

3. Aon recognizes that cybersecurity is essential to businesses that collect and maintain sensitive information on their own behalf or on behalf of others. Aon offers to evaluate the cybersecurity risk profile of its clients and promotes its CyQu Enterprise product, a cyber risk assessment platform designed to identify internal data security practices and remediate risks therein.[4]

4. Aon also offers assistance to companies affected by data breach incidents and recognizes the importance of keeping PII and other sensitive data secure.[5] For example, as part of its effort to promote its cyber insurance product, Aon highlights the consequence of lax cyber security practices, "[a] cyber breach has the potential to interrupt business operations, supply chains, products, and beyond. It can also impact third parties such as clients, patients, or guests."[6]

5. According to its website, Aon is the "Go To Cyber Response Team"[7] Aon represents its extensive experience and preparedness in data security practices.

> We have been the go-to firm for organizations and their law firms in investigating ninety percent of the highest profile breaches in the last decade. This experience, together with our advanced threat intelligence capabilities, means we know the latest attack vectors, how cyber attacks are perpetrated, and how to stop them..."[8]

6. Despite Aon's proclaimed expertise in the area of cybersecurity and its acknowledgement of the risk that companies like itself and its clients face, Aon failed to detect an unauthorized intrusion into its systems for over a year. From December 2020, to February 6, 2022 an unknown actor had access to certain segments of Aon's network, including segments that contained the PII of Plaintiff and Class Members (the "Data Breach").

---

[4] https://www.aon.com/cyber-solutions/cyqu-cyber-quotient-evaluation/
[5] *See* https://www.aon.com/cyber-solutions/breach-assistance-contact/.
[6] https://www.aon.com/cyber-solutions/solutions/cyber-insurance/
[7] *See* https://www.aon.com/cyber-solutions/solutions/cyber-security-testing/.
[8] *Id.*

7. During the Data Breach, the attacker accessed records that contained the personal information of approximately 145,000 individuals.

8. It was only on or around February 25, 2022 that Defendant finally detected the year-long intrusion underlying the Data Breach.

9. On or around May 27, 2022, more than three months after it detected the Data Breach, Defendant finally began notifying some Class Members that their PII had been accessed by an unauthorized intruder. Defendant delayed in noticing affected individuals despite itself understanding the need to act quickly to mitigate the fallout of a cyber event like the one it experienced. Defendant even instructs potential clients that "[c]yber security threats are growing in volume and complexity. When facing an attack, time is of the essence."[9][10]

10. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the PII impacted during the Data Breach included at least Social Security numbers, driver's license information, and/or benefit enrollment information.

11. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

12. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to

[9] https://www.aon.com/cyber-solutions/solutions/incident-response-retainer/
[10] https://www.aon.com/cyber-solutions/breach-assistance-contact/: "During a breach, you need to act fast. Our response teams are available 24/7."

Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited several months to report it to affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information.

13. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

14. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

15. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and substantially increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

16. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

17. Plaintiff Misty Williams is a Citizen of Florida residing in Okaloosa County, Florida.

18. Defendant Aon PLC is a corporation organized under the laws of Ireland, and its United States headquarters, nerve center, and principal place of business is located at 200 E. Randolph St. in Chicago, Illinois. Defendant Aon PLC's U.S. headquarters occupies floors 3 to 15 in the Aon Center building, Chicago's fourth largest skyscraper.

19. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

20. All of Plaintiff's claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

22. The Northern District of Illinois has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Illinois and this District through their headquarters, offices, parents, and affiliates.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

24. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

25. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

26. Defendant's Global Privacy Policy ("Privacy Policy") recognizes that Aon had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

27. Defendant's Privacy Policy applies to any personal information provided to Aon and any personal information that Aon collects from other source."[11] Aon's Privacy Policy also represents:

> The security of your personal information is important to us and Aon has implemented reasonable physical, technical and administrative security standards in an effort to protect personal information from loss, unauthorized access, misuse, alteration or destruction and to ensure that such information is processed in accordance with applicable data privacy laws.[12]

28. Regarding the deletion of personal information Defendants no longer need, the Privacy Policy represents as follows:

> How long we retain your personal information depends on the purpose for which it was obtained and its nature. We will keep your personal information for the period necessary to fulfil the purposes described in this Statement unless a longer retention period is permitted or required by law and in accordance with the Aon Record Retention Policy. Your personal information will be securely destroyed when it is no longer required.[13]

The Data Breach

29. On or about May 27, 2022, Defendant sent Plaintiff and Class Members a Notice of Data Breach.[14] Defendant also notified various state Attorneys General of the Data Breach and provided the Attorneys General with "sample" notices of the Data Breach. The Notice of Data Breach informed Plaintiff and Class Members (in substantially the same form) that:

---

[11] *See* https://www.aon.com/about-aon/privacy.jsp

[12] *Id*.

[13] *Id*.

[14] *See, e.g.,* https://oag.ca.gov/ecrime/databreach/reports/sb24-553817

> **What Happened?** On February 25, 2022, Aon identified a cyber incident that, upon investigation, impacted a limited number of systems. Once the incident was discovered, Aon immediately retained leading cybersecurity firms to assist in responding and help conduct a thorough investigation of the incident. The investigation revealed that an unauthorized third party accessed certain Aon systems at various times between December 29, 2020 – February 26, 2022. Findings from the investigation indicate the unauthorized third party temporarily obtained certain documents containing personal information from Aon systems during this period. Aon has taken steps to confirm that the unauthorized third party no longer has access to the data and Aon has no indication the unauthorized third party further copied, retained, or shared any of the data. We have no reason to suspect your information has or will be misused.
>
> **What Information Was Involved?** Aon reviewed the data that was obtained and determined it contained some of your personal information, including your name and one or more of the following: Social Security number, driver's license number, and, in a small number of cases, benefit enrollment information.
>
> **What Are We Doing.** Aon immediately reported the incident to, and is working closely with, law enforcement authorities, including the FBI. Additionally, to prevent a similar occurrence in the future, we implemented numerous measures designed to enhance the security of our network, systems, and data. Aon will continue to evaluate additional steps that may be taken to further enhance the firm's security environment.[15]

30. Defendant advised that the information potentially impacted in the Data Breach included Social Security numbers, driver's license information, and/or benefits enrollment information.[16]

31. Defendant admitted in the Notice of Data Breach, the reports to the Attorneys General, and the "sample" notices of the Data Breach, that unauthorized third persons accessed files that contained sensitive information about Plaintiffs and Class Members.

---

[15] *Id.*

[16] *Id*.

32. And there is a potential that more information was accessed and exfiltrated during the more than a year that the attacker was able to access Defendant's system without detection. Aon collects a wide range of PII and other sensitive data as part of its regular business. Aon informs individuals whose information it that it maintains:

- Basic personal details, such as your name, address contact details, date of birth, age, gender and marital status;
- Unique identifiers such as National Insurance Number or pension scheme reference number;
- Demographic details, such as information about your age, gender, race, marital status, lifestyle, and insurance requirements;
- Employment information such as role, employment status (such as full/part time, contract), salary information, employment benefits, and employment history;
- Health information such as information about your health status, medical records and medical assessment outcomes;
- Benefits information such as benefit elections, pension entitlement information, date of retirement and any relevant matters impacting your benefits such as voluntary contributions, pension sharing orders, tax protections or other adjustments;
- Financial details such as payment card and bank account details, details of your credit history and bankruptcy status, salary, tax code, third-party deductions, bonus payments, benefits and entitlement data, national insurance contributions details;
- Claims details such as information about any claims concerning your or your employer's insurance policy;
- Your marketing preferences;
- Online information: e.g., information about your visits to our websites;
- Events information such as information about your interest in and attendance at our events, including provision of feedback forms;
- Social media information such as interactions (e.g., likes and posts) with our social media presence; and
- Criminal records information such as the existence of or alleged criminal offences, or confirmation of clean criminal records.[17]

[17] https://www.aon.com/about-aon/privacy.jsp

33. Defendant claims that "to prevent a similar occurrence in the future, we implemented numerous measures designed to enhance the security of our network, systems, and data.."[18] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected. There is a strong potential that additional information could have been accessed or that further breaches could occur.

34. Nor has Defendant properly informed Plaintiff and Class Members of the scope of the breach. By stating only that the intruder accessed "benefit enrollment information," they omit that such information includes, "benefit elections, pension entitlement information, date of retirement and any relevant matters impacting [] benefits such as voluntary contributions, pension sharing orders, tax protections or other adjustments." This is a wide array of information that can be utilized by an actor to better commit identity theft or financial crimes.[19]

35. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII for approximately 145,000 individuals.

[18] https://oag.ca.gov/ecrime/databreach/reports/sb24-553817

[19] https://www.aon.com/about-aon/privacy.jsp

37. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[20]

38. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders

[20] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

39. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

[21] *Id.* at 3-4.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[22]

40. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs

[22] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[23]

41. Given Defendant's own cybersecurity expertise and that Defendant stored the PII of hundreds of thousands of individuals—and likely much more than that--Defendant could and should have implemented all of the above measures to prevent and detect and prevent cyber intrusions.

42. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII f more than 145,000 individuals, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

43. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members for its own pecuniary gain.

44. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

45. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely

[23] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

46. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members.

47. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts made by and directed to companies like Defendants to protect and secure sensitive data they possess. Defendant's negligence is further exacerbated by its failure to heed its own warnings, replete through its marketing and promotional materials.

48. Defendant published an article titled, *Preparing For The Expected: Cyber Incidents & Data Breaches*,[24] in which it states, "an effective cyber security strategy starts with the belief that prevention is always better than cure." Defendant goes on to describe the sophistication of attackers, the increasing frequency of cyber intrusions, and identifies businesses like itself as particularly susceptible to cyber threats. Defendant even poses the question, "Have the doors been left unlocked to cyber-attackers?"

49. Despite this knowledge and the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

50. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25]

[24] https://www.aon.com/cyber-solutions/thinking/preparing-for-the-expected-cyber-incidents-data-breaches/
[25] 17 C.F.R. § 248.201 (2013).

The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[26]

51. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

52. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[27] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[28] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[29]

53. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult

---

[26] *Id*.

[27] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Oct. 27, 2021).

[28] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Oct. 27, 2021).

[29] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 27, 2021).

for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[30]

54. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

55. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

56. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

[30] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 27, 2021).

[31] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Oct. 27, 2021).

breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

57. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[32]

58. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

59. The fraudulent activity resulting from the Data Breach may not come to light for years.

60. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[33]

61. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can

[32] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 23, 2021).

[33] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021)

> provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[34]

62. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[35] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[36]

63. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[37]

64. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

---

[34] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021)

[35] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)

[36] *Id.*

[37] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

65. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.[39]

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

67. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

68. To date, Defendant has offered Plaintiff and Class Members only two years of identity and credit monitoring services through Experian IdentityWorks. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services.

---

[38] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

[39] *See* https://www.aon.com/cyber-solutions/solutions/cyber-impact-analysis/:

> A data breach could cost your organization $3.86 million on average and recent ransomware losses were in the hundreds of millions. The economic impact from cyber events can threaten the financial health of your organization and its ability to operate sustainably.

69. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Misty William's Experience

70. Plaintiff is an employee of Asurion, a company that contracts with Aon to provide it with benefit administration services.

71. In connection with her employment with Asurion, was required to and did Plaintiff entrust her PII to Defendant.

72. At the time of the Data Breach (December 2020 to February 2021), Defendant retained at least Plaintiff's social security number, driver's license information, and benefit enrollment information in its system.

73. Plaintiff received Defendant's Notice of Data Breach, dated May 27, 2022 on or about that date. The notice stated that Plaintiff's social security number, driver's license information and benefit enrollment information were among the information accessed or acquired during the Data Breach.

74. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

75. Plaintiff also suffered from the misuse of her PII when someone, almost certainly using her PII that was exfiltrated in the Data Breach, attempted to process a $499.99 charge to her PayPal account. It should be assumed that Plaintiff's PII and that of the Class has been offered for sale on internet marketplaces and will be used again.

76. Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

77. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

78. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

79. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

80. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and criminals.

81. Plaintiff has also experienced a substantial increase in suspicious telephone calls, emails, and text messages which she believes is related to her PII being placed in the hands of unauthorized third parties and possibly criminals in the Data Breach.

82. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

83. Plaintiff bring this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

84. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All United States residents whose PII was accessed or acquired during the cyber intrusion that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around May 27, 2022 (the "Nationwide Class").

85. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff assert claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Florida whose PII was accessed or acquired during the cyber intrusion that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around May 27, 2022 (the "Florida Subclass" collectively with the Nationwide Class the "Classes").

86. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

87. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

88. Numerosity, Fed R. Civ. P. 23(a)(1): The members of the Classes are so numerous that joinder of all members is impracticable. Defendant has identified approximately 145,000 individuals whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

89. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

90. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

91. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

92. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel

experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

93. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

94. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

95. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

96. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

97. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

98. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

99. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Florida Subclass)

100. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs. Plaintiff brings this Count on behalf of herself and the Nationwide Class or, alternatively, the Florida Subclass (collectively herein, the "Classes").

101. Plaintiff and the Classes entrusted Defendant with their PII.

102. Plaintiff and the Classes entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

103. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Classes could and would suffer if the PII were wrongfully disclosed.

104. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Classes involved an unreasonable risk of harm to Plaintiff and the Classes, even if the harm occurred through the criminal acts of a third party.

105. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

106. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII once they were no longer required to retain pursuant to regulations.

107. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Classes.

108. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Classes. That special relationship arose because Plaintiff and the Classes entrusted Defendant with their confidential PII, a necessary part of obtaining benefits from their employers or services from Defendant.

109. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Classes.

110. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Classes was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

111. Plaintiff and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Classes, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

112. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Classes. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Classes, including basic encryption techniques freely available to Defendant.

113. Plaintiff and the Classes had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

114. Defendant wase in a position to protect against the harm suffered by Plaintiff and the Classes as a result of the Data Breach.

115. Defendant has and continues to have a duty to adequately disclose that the PII of Plaintiff and the Classes within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

116. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Classes.

117. Defendant has admitted that the PII of Plaintiff and the Classes was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

118. Defendant, through its own actions and/or omissions, unlawfully breached its duties to Plaintiff and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Classes during the time the PII was within Defendant's possession or control.

119. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

120. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Classes in the face of increased risk of theft.

121. Defendant, through its own actions and/or omissions, unlawfully breached its duty to Plaintiff and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

122. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII it was no longer required to retain pursuant to regulations.

123. Defendant, through its own actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Classes the existence and scope of the Data Breach.

124. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Classes, the PII of Plaintiff and the Classes would not have been compromised.

125. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Classes was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

126. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

127. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Classes.

128. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

129. Plaintiff and the Classes are within the class of persons that the FTC Act was intended to protect.

130. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

131. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Classes; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Classes.

132. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

133. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

134. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Classes are entitled to recover actual, consequential, and nominal damages.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class
or, alternatively, the Subclass and in the Alternative to all other Counts)

135. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs. Plaintiff brings this Count on behalf of herself and the Nationwide Class or, alternatively, the Florida Subclass (collectively herein, the "Classes"). Plaintiff pleads this Count in the alternative to all other Counts alleged herein.

136. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

137. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

138. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

139. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

140. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

141. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

142. Plaintiff and Class Members have no adequate remedy at law.

143. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

144. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

145. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT III
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

146. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs. Plaintiff brings this Count on behalf of herself and the Nationwide Class (the "Class" for purposes of this Count).

147. Plaintiff and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff and the Class, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

148. Defendant is engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engaged in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

149. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Class's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and

security measures and protect Plaintiff and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

150. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

151. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

152. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

153. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

154. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

155. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity

theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff and the Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

156. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT IV
Violation of Florida's Unfair and Deceptive Trade Practices Act
(On Behalf of Plaintiff and the Florida Subclass)

157. Plaintiff re-alleges and incorporates by reference herein all of the preceding allegations. Plaintiff brings this Count on her own behalf and that of the Florida Subclass (the "Class" for the purpose of this Count).

158. The Florida Unfair and Deceptive Trade Practices Act (hereinafter "FUDTPA") is expressly intended to protect "consumers" like Plaintiff and Class Members from unfair or deceptive trade practices.

159. Plaintiff and Class Members have a vested interest in the privacy, security and integrity of their PII, therefore, this interest is a "thing of value" as contemplated by FUDTPA.

160. Defendant is a "person" within the meaning of the FUDTPA and, at all pertinent times, was subject to the requirements and proscriptions of the FUDTPA with respect to all of its business and trade practices described herein.

161. Plaintiff and Class Members are "consumers" "likely to be damaged" by Defendant's ongoing deceptive trade practices.

162. Defendant's unfair conduct as described in this Complaint, was directed, and emanated from Defendant's U.S. headquarters to the detriment of Plaintiff and Class Members in Florida and throughout the United States.

163. Defendant engaged in unfair and deceptive trade practices because it creates a reasonable expectation of privacy to all Florida consumers promising to keep consumers PII safe, but then failed to take commercially reasonable steps to protect the PII with which it is entrusted.

164. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of FDUTPA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Class's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

165. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable

state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

166. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

167. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

168. Defendant also violated FDUTPA by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to Fl. Stat. 817.5681(1)(a) et seq.

169. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

170. As a direct and proximate result of Defendant's violations of FDUTPA, Plaintiff and the Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff and the Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and

other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

171. Plaintiff and Class Members have suffered ascertainable losses as a direct result of Defendants' employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

172. Under FDUPTA, Plaintiff and the Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff and the Class seek equitable relief and to enjoin Defendant on terms that the Court considers appropriate.

173. Defendant's conduct caused and continues to cause substantial injury to Plaintiff and Class Members. Unless preliminary and permanent injunctive relief is granted, Plaintiff and the Class will suffer harm, Plaintiff and the Class do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiff and the Class.

174. At all material times, Defendant's unfair and deceptive trade practices were willful within the meaning of FUDTPA and, accordingly, Plaintiff and the Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

COUNT V
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, the Subclass)

175. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs. Plaintiff brings this Count on behalf of herself and the Nationwide Class (the "Class" for purposes of this Count).

176. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

177. Defendant owed a duty to Plaintiff and Class Members to keep their PII contained as a part thereof, confidential.

178. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiff and Class Members.

179. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

180. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

181. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their relationships with Defendant or Defendant's clients, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

182. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Member's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

183. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

184. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

185. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

186. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Florida Subclass and appointing Plaintiff and her Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant's to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: June 29, 2022

Respectfully Submitted,

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
Email: gklinger@milberg.com

/s/ Patrick N. Keegan
Patrick N. Keegan*
KEEGAN & BAKER, LLP
2292 Faraday Avenue, Suite 100
Carlsbad, CA 92008
Telephone: 760-929-9303
Fax: 760-929-9260
Email: pkeegan@keeganbaker.com

**pro hac vice application forthcoming*

/s/ *Ryan A. Stygar*
Ryan A. Stygar*
CENTURION TRIAL ATTORNEYS, APC
8880 Rio San Diego Dr., Suite 800
San Diego, CA 92108
Telephone: (858) 206-8833
Fax: (760) 753-3206
Email: ryan@centurionta.com

**pro hac vice application forthcoming*